GIPSON HOFFMAN & PANCIONE
A Professional Corporation
GREGORY A. FAYER (State Bar No. 232303)
GFayer@ghplaw.com
ELLIOT B. GIPSON (State Bar No. 234020)
EGipson@ghplaw.com
1901 Avenue of the Stars, Suite 1100
Los Angeles, California 90067-6002
Telephone: (310) 556-4660
Facsimile: (310) 556-8945

Attorneys for Plaintiff
CYBERsitter, LLC d/b/a Solid Oak Software

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA - SOUTHERN DIVISION

CYBERsitter, LLC, a California limited liability company, d/b/a Solid Oak Software,

Plaintiff,

v.

The People's Republic of China, a foreign state; Zhengzhou Jinhui Computer System Engineering Ltd., a Chinese corporation; Beijing Dazheng Human Language Technology Academy Ltd., a Chinese corporation; Sony Corporation, a Japanese corporation; Lenovo Group Limited, a Chinese corporation; Toshiba Corporation, a Japanese corporation; ACER Incorporated, a Taiwanese corporation; ASUSTeK Computer Inc., a Taiwanese corporation; BenQ Corporation, a Taiwanese corporation; Haier Group Corporation, a Chinese corporation; DOES 1-10, inclusive,

Defendants.

CASE NO. CV 10-00038 JST (SH)

DECLARATION OF DR. J. ALEX HALDERMAN IN SUPPORT OF PLAINTIFF'S OPPOSITION TO MOTION OF DEFENDANT SONY CORPORATION TO DISMISS THE ACTION ON GROUNDS OF *FORUM NON CONVENIENS* AND RELATED JOINDERS

Judge: Hon. Josephine Staton Tucker
Ctrm: 10A

Hearing Date: Nov. 8, 2010
Hearing Time: 10:00 a.m.

Discovery Cutoff: None Set
Pretrial Conference: None Set
Trial Date: None Set

DECLARATION OF DR. J. ALEX HALDERMAN

I, Dr. J. Alex Halderman, declare as follows:

1. I, J. Alex Halderman, submit the following declaration in support of the opposition of plaintiff CYBERsitter, LLC d/b/a Solid Oak Software ("Plaintiff") to the motion of defendant Sony Corporation ("Sony") to dismiss the action on grounds of *forum non conveniens* ("Motion") and to the joinders of ACER Incorporated ("Acer"), ASUSTeK Computer Inc. ("Asus") and BenQ Corporation ("BenQ") (collectively, "Defendants").

My Background and Qualifications

2. My name is J. Alex Halderman. I am an assistant professor of electrical engineering and computer science at the University of Michigan, where I have been on the faculty for about two years. I received my Ph.D., M.A., and A.B. from Princeton University in 2009, 2005, and 2003, respectively. I continue to hold a visiting appointment at Princeton's Center for Information Technology Policy.

3. I have been involved in computer science research and teaching since 2001. I have published nineteen papers in the academic literature, two of which received best paper awards at the conferences where they were presented. I created Michigan's undergraduate computer security course and redesigned its graduate computer security course, and I teach both regularly. I have served on the program committees of more than fourteen academic conferences and workshops. I am a member of the Association for Computing Machinery and of USENIX, the Advanced Computing Systems Association.

4. I have extensive experience with analysis of deployed software, hardware, and systems. Much of my research has focused on understanding and comparing the behaviors of complex closed-source products, such as electronic voting machines and digital rights management systems. My work in these areas has received international media attention.

Discovery of the Copying of CYBERsitter Code in Green Dam Program

5. I have been investigating the Green Dam software as part of my academic research for more than 16 months. It first came to my attention at the beginning of June 2009, when a colleague in China told me that the Chinese government planned to require PC makers to distribute the software. Shortly thereafter, I began to analyze Green Dam's functionality and security, with assistance from my PhD student Scott Wolchok and from undergraduate computer science major Randy Yao.

6. We initially examined a copy of Green Dam that we obtained as a free download from www.lssw365.net, the official distribution website. Within hours, we discovered that Green Dam contained numerous security flaws due to widespread programming errors by its developers. Some of these vulnerabilities were extremely dangerous, because malicious web sites could exploit them to seize control of the user's PC. Once in control, a malicious site could steal private data or make use of the computer for further crimes, such as sending spam email or launching attacks on other systems or networks.

7. We also investigated Green Dam's content filtering mechanisms. When a user attempts to visit a web page, Green Dam intercepts the request and examines the server name and the address of the page. It determines whether the request should proceed by applying thousands of rules, which are contained in a set of filter files included with the software.

8. The Green Dam developers used encryption to conceal the contents of approximately one third of the program's files, including all of the filter files. In order to analyze the filters, my students and I needed a way to decrypt them. We determined that the encryption scheme is a simple scrambling process that does not involve any secret keys, and we were able to develop a tool that unscrambles the file contents.

9. When we decrypted the Green Dam files, we found evidence that many of them had been copied from CYBERsitter. Specifically, we noticed that Green Dam includes an encrypted configuration file that references the names of the filters together with locations on a Solid Oak web site where the corresponding CYBERsitter filters can be downloaded. We also discovered that a second encrypted file distributed with Green Dam contains announcements that were apparently sent by Solid Oak to CYBERsitter customers in 2004. Another Green Dam file indicates that the developers stored the filters in a folder named "2006data" prior to shipping them to users. From this we conjectured that the filters were copied from CYBERsitter at some time in 2006.

10. We publicly announced these findings on June 11, 2009, in a technical report entitled "Analysis of the Green Dam Censorware System." The Green Dam developers quickly responded by making changes to the software, which we analyzed in an addendum to our report dated June 18, 2009. Since that time, I have been monitoring additional changes to the software as they have been published.

11. Brian Milburn, President of Solid Oak Software, contacted me on June 12, 2009—the day after these findings became public—and offered to assist me in my analysis of the copied files. At my request, he provided a version of the CYBERsitter software that dates from around the time of the suspected copying, and a tool for decrypting the CYBERsitter filters. I subsequently performed extensive comparative analysis of the Green Dam and CYBERsitter products.

Results of Comparative Analysis and Evidence of Copying

12. Except where otherwise noted, my analysis in this section compares the version of Green Dam that I downloaded from the www.lssw365.net web site on June 8, 2009 and the version of CYBERsitter provided to me by Brian Milburn on June 15, 2009. The Green Dam software is labeled version 3.17 and appears to have been released on or around June 1, 2009. The CYBERsitter software is labeled version

9.7.1.21 and appears to have been released about two years earlier, on or around July 17, 2007.

13. By decrypting the Green Dam files, I determined that the software includes 35 files that contain filter rules. Of these, 33 specify different categories of prohibited requests ("filters"), and the remaining two specify exceptions to the prohibitions ("whitelists"). My testing indicates that Green Dam actually applies rules from only five of the filters and one of the whitelists (the "active filters" and "active whitelist"). The remaining 28 filters and one whitelist have no apparent role in the operation of the software (the "inactive filters" and "inactive whitelist").

14. Green Dam contains several other files that have similar filenames to the filters and whitelists (ending in ".dat") and that are encrypted in the same manner. After decrypting these files, I found that one of them (wfileu.dat) is a filter index that contains descriptions and other data about 28 filters. Each filter is listed with a filename that ends with ".dll", the naming convention used in CYBERsitter, rather than with the Green Dam convention that ends files with ".dat". Other than this difference, the listed filters all correspond to filter files installed by Green Dam, including four of the five active filters and 24 of the 28 inactive filters.

15. The index also lists a web page address for each filter. These addresses are all on the web site cybersitterfiles.com, which is operated by Solid Oak and used to distribute updated copies of the CYBERsitter filters to licensed CYBERsitter users. Here are the first four entries from the decrypted file:

1|Default|Adult/Sexually Oriented|adwfil.dll|80|http://cybersitterfiles.com/adwfil.dll

1|Default|Illegal Activities/Drugs|iawfil.dll|80|http://cybersitterfiles.com/iawfil.dll

1|Default|Hate/Intolerance|hatfil.dll|80|http://cybersitterfiles.com/hatfil.dll

1|Default|Illegal Guns/Violence|viofil.dll|80|http://cybersitterfiles.com/viofil.dll

16. The file appears to serve no purpose in Green Dam, but the CYBERsitter software includes a correspondingly named file (wfileu.drv) that it actively uses as a catalog of available filters. I compared the decrypted contents of the Green Dam file

with the decrypted contents of the corresponding CYBERsitter file and found that all 28 filter descriptions in the Green Dam file were contained in exactly the same form in the CYBERsitter file.

17. Green Dam includes another file (bsnlst.dat) that contains ten 16-digit numbers in encrypted form. The version of CYBERsitter that I examined contains a corresponding file (bsnlst.dll) with exactly the same decrypted contents. This file appears to serve no purpose in Green Dam, but the CYBERsitter software uses it to store a list of product serial numbers that have been deactivated.

18. Another file that is distributed included in the Green Dam software (csnews.dat) contains an encrypted form of the following text:

> May 10, 2004
>
> CYBERsitter Version 9 released. This is a free upgrade and is available at:
>
> http://www.getcybersitter.com
>
> May 4, 2004
>
> If you haven't got a SpyWare checker for your computer yet, now is the time. SpyWare is installed by numerous freely downloaded programs, especially peer to peer file and music sharing programs. These types of programs can literally turn your computer into an unusable machine. It can cost you hundreds of dollars in repair costs. Our best advice: Never download file or music sharing programs. Always read every single word on the screen when installing a free program from the internet. If you see anything that indicates that the program is going to install any additional "enhancement" programs, abort the installation immediately. For more information on SpyWare, how to prevent it, and how to get rid of it, please visit:
>
> http://www.cybersitterhelp.com

19. This text appears to be an announcement that Solid Oak sent to CYBERsitter users via that software's filter update delivery mechanism. It serves no purpose in Green Dam.

20. These three files have no apparent purpose in Green Dam, but they have clear functions in CYBERsitter. One is identical to a file found in CYBERsitter and the others are filled with references to the name "CYBERsitter." The only plausible explanation is that these files were copied from CYBERsitter to Green Dam.

21. Four of the five filters that are actively used by Green Dam correspond to files with similar names in the version of CYBERsitter I examined. I performed a rule-by-rule comparison of each pair of filters. One of the active Green Dam filters (iawfil.dat) consists entirely of rules found in the corresponding CYBERsitter filter. For the three others (lgwfil.dat, vgamfil.dat, and adwfil.dat), I found that 90-96% of their rules were contained in the corresponding CYBERsitter filters. In each case, Green Dam expresses these rules in the same way, and in the same order, as CYBERsitter. Overall, 2091 of the 2287 rules (91%) in the four Green Dam filters were present in the CYBERsitter filters.

22. The Green Dam filters with correspondingly named CYBERsitter filters all have file creation dates of September 8, 2006, except for one of the active filters (adwfil.dat), which has a creation date of December 31, 2007. If the creation dates accurately reflect the dates of two instances of copying, the CYBERsitter filters that I examined, which appear to date from around July 17, 2007, are from 11 months later and five months earlier.

23. Solid Oak, like many makers of filtering software, frequently revises its filter rules to keep them up-to-date as content on the Internet changes. Therefore, unless we compare the Green Dam filters to the CYBERsitter filters from the exact revision when copying occurred, we should expect there to be some number of differences even if the Green Dam developers made no subsequent modifications.

24. Given the complexity of the filter rules and the creativity and judgment involved in their design, it would be impossible for the two programs to have this many identical filter rules by chance. The only plausible explanation is that these filters were copied.

Changes in Later Green Dam Versions and Current Distribution

25. On June 11, 2009, I released a brief technical report describing the security problems and evidence of copying that my students and I found in our initial investigation of Green Dam. Within days, the Green Dam developers responded by making a series of changes to the software.

26. On or about June 13, the Green Dam developers replaced the installation file on the www.lssw365.net download site with a revised version. I am not aware of any public announcement or indication of this change, and the revised Green Dam bears the same version number as the release it replaced, 3.17. To distinguish the two, I will refer to the original release as Green Dam 3.17 and the revised release as Green Dam 3.17a.

27. Green Dam 3.17a contains two notable changes. First, it corrects the immediate security problem that my students and I highlighted. (However, we discovered that it is vulnerable to other, related problems.) Second, it omits 35 files that were present in the original 3.17 version. At least 32 of these files appear to have been copied from CYBERsitter, including 28 filters and one whitelist that together contain more than 6000 rules. None of these 32 files seems to serve any functional purpose in Green Dam 3.17.

28. In contrast, the four filters copied from CYBERsitter that are actively used in Green Dam 3.17 continue to be distributed, installed, and actively used in Green Dam 3.17a. The Green Dam developers did not change a single rule in these filters when they revised the program.

29. Users running Green Dam 3.17 are not automatically affected by the release of 3.17a. If a 3.17 user downloads and installs 3.17a manually, it will apply the security fixes, but all the CYBERsitter files will remain installed unless the user uninstalls Green Dam 3.17 prior to installing the new version.

30. The Green Dam software includes a "filter update" feature that can retrieve and install the latest content filters and other components from a location on the zzjinhui.com web site. In the week after I published my technical report, the Green Dam developers released two updates using this system.

31. The first filter update, version F3.173, was released on or around June 12, 2009. Its main effect is to disable the four actively filters copied from CYBERsitter. After the update is applied, Green Dam no longer uses rules from these filters, although the filter files remain on the user's system. Only one filter, adwapp.dat, remains active and listed in the Green Dam settings window.

32. With the CYBERsitter filters disabled, Green Dam's content filtering loses much of its effectiveness. I found that the remaining filter, which does not appear to be copied from CYBERsitter, permits searchers for "porn" and access to addresses containing the terms "sex" and "porn." Surprisingly, it does block access to columbia.edu and cybersitter.com.

33. The Green Dam developers released a second filter update, version F3.174, on or around June 16. This update replaces only a single file, the "help" file that provides instructions for users (kw.chm).

34. While filter update F3.173 does disable the copied filters (as my students and I observed in an addendum to our report on June 18), it likely only affected a small fraction of Green Dam users. The Green Dam filter update mechanism is designed to provide users the most up-to-date revision of content filters, so it only applies the newest update that's available. As a result, Green Dam users only received the F3.173 update if their software checked for filer updates during the approximately four-day window between the time when F3.173 was released and the time when it was superseded by the release of F3.174. This is unlikely to be a large fraction of users, given that Green Dam does not check for updates automatically unless the user explicitly configures it to do so.

35. I have examined a number of filter updates released subsequently, including the current filter update, F3.180, which was released on or around March 17, 2010, and I have seen no evidence that the Green Dam developers reissued filter removal instructions in a later update. The CYBERsitter filters are likely still active for any Green Dam 3.17 or 3.17a user who did not perform a filter update during that short time in June 2009.

36. As of October 10, 2010, the Green Dam installation file distributed as a free download from the lssw365.net web site is still version 3.17a, which contains, installs, and actively uses four filters copied from CYBERsitter. These filters remain active even if the user applies the current filter update, F3.180.

37. The 3.17a and F3.173 updates precise target the set of files that my analysis above indicates were copied from CYBERsitter, and filter update F3.173 demonstrates that the Green Dam developers have the ability to deactivate the copied filters for at least a portion of the user base. For whatever reason, the developers chose not to exercise this ability going forward, and as a result, almost all copies of Green Dam 3.17 or 3.17a that have been installed since approximately June 16, 2009 (when F3.173 was superseded) likely have the copied filters enabled.

Evidence Relevant to Copying and Intent to Copy

38. In my experience and opinion, based on my training and comparative analysis of tens of software programs, copying in cases such as this must be determined and verified through a direct examination of the physical evidence at issue – namely, through a line-by-line expert analysis of the contents of the software programs in question. The evidence of copying lies in the programs themselves, and is apparent from the contents of the programs themselves regardless of what the particular individuals allegedly involved in the development or dissemination of the programs might have to say about them.

39. This is particularly so in cases such as this involving such extensive copying as I have found here, where there are thousands of identical rules in the two

programs. Under these circumstances, there is little or nothing that non-expert testimony could add to the analysis of the programs.

40. In my experience and opinion, such widespread copying as I have found here could not result from mere inadvertence or accident, but would clearly require an intentional act on the part of the program developers. Thus, unlike cases in which there may be a slight overlap or minor similarities in coding that might be explained by inadvertence or accident, the testimony of the Green Dam developers could have no conceivable bearing on the issues of copying and intent to copy here. The intent to copy is evident here from an analysis of the programs themselves. The intentional nature of the copying is clear both from the scope of the copying and from the manner in which portions of the copied code are integrated into the Green Dam program in a manner that allows useful functioning of the copied code in the context of the program. Thousands of rules do not accidentally or inadvertently leap from one program into another, nor do they accidentally or inadvertently integrate themselves into the new program in an executable manner.

Expert's Personal Concerns Regarding Travel

To the best of my knowledge, my Green Dam technical report was the first publication to expose the software's deep-rooted security problems and blatant copying. These revelations helped fuel the backlash against Green Dam within China and set off a chain of events that ultimately brought about the retraction of the government mandate. As a consequence of my role in these events, I am deeply concerned that traveling to China, particularly in my capacity as technical expert in

this case, would expose me to unacceptable risks of reprisal and jeopardize my personal safety.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on October 11, 2010, at Ann Arbor, Michigan.

Dr. J. Alex Halderman